

Appl. No. : 09/698507
Filed : October 26, 2000

REMARKS

By this paper, Claim 1, 7, 16, 17, 24, 25, 36, 37, 38, 44, 49, 55, 58, and 68 have been amended. Claims 2-6, 8-15, 18-23, 26-35, 39-43, 45-48, 50-54, 56-57, and 59-67 remain unchanged. Thus, Claims 1-70 remain pending in the application and are presented for further examination.

I. Rejection of Claim 7 under 35 U.S.C. § 112

In paragraph 4 of the amendment, the Examiner rejected Claim 7 for failing to have sufficient antecedent based for “said asymmetric keys.” Applicant has amended Claim 7 to depend from Claim 6. Applicant therefore submits that Claim 7 is in condition for allowance.

II. Rejection of Claims 1-70 under 35 U.S.C. § 103(a)

In paragraph 6 of the Office Action, the Examiner rejected Claims 1-70 as being unpatentable over U.S. Patent Number 6,233,577 to Ramasubramani, et al (“Ramasubramani”) in view of U.S. Patent No. 5,762,552 to Vuong, et al. (“Vuong”). The Examiner took the position that Ramasubramani teaches all limitations of Claims 1-70 except that Ramasubramani “does not specifically teach the client server to be a gaming machine and a gaming server. However, [Vuong] teaches a gaming machine and a gaming server.” *Office Action* at 6. For the reasons set forth below, Applicant submits that the claims would not have been obvious in view of cited references.

A. Brief Description of One Embodiment

One claimed embodiment includes a gaming server that receives requests to initiate game play from a remote machine. *Specification* at 8. The gaming server provides encryption keys to a gaming machine. *Specification* 11-12. The gaming machine (which is configured to determine the outcome of game play) uses those keys to encrypt communication of gaming related information such as player credit card, player identification, wagering, and casino payout information with the remote machine. *Id.* Thus, management and generation of keys is centrally managed and performed by the gaming server. However, encryption of gaming related information is performed on the gaming machine for transmission to the remote machine. *Specification* at 12.

Appl. No. : 09/698507
Filed : October 26, 2000

B. Law of Obviousness

To establish a *prima facie* case of obviousness, three basic criteria must be met: (1) there must be some suggestion or motivation to combine the reference teachings, (2) there must be a reasonable expectation of success, and (3) the references when combined must teach or suggest all of the claim limitations. *See M.P.E.P. § 2143*. It is well settled that “a showing of a suggestion, teaching or motivation to combine the prior art references is an ‘essential component of an obviousness holding.’” *See, e.g., Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 U.S.P.Q.2d 1456, 1459 (Fed. Cir. 2000). The Examiner can satisfy the burden of showing obviousness of the combination “only by showing some objective teaching in the prior art or knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references.” *In re Fitch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992). “Determination of obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention.” *ATD Corp. v. Lydall, Inc.*, 159 F.3d 534, 546 (Fed. Cir. 1998).

C. Brief Overview of *Ramasubramani*

Ramasubramani discloses a system in which a proxy server handles certificate and encryption management for thin client devices that connect to a secure web server (e.g., via HTTPS) via the proxy server. *See e.g., Ramasubramani* at Figure 3. A first secure protocol, e.g., HDTTP, is used by the mobile device (what the Examiner equates to the “gaming machine” of the claimed invention) to communicate with the proxy server (what the Examiner equates to the “gaming server” of the claimed invention). *Id.* A second protocol, e.g., HTTPS is used to communicate between the proxy server and the business server. *Id.* and Figure 4A. As described with reference to Figures 6A and 6B, the keys and certificates managed by the proxy server are related to this second protocol. *Ramasubramani*, col. 12, lines 63 – col. 13, lines 1-11, col. 14, lines 18-41. The proxy server thus communicates via the second protocol with secure web server using encryption keys that it maintains while communicating with the thin client via the first protocol. *Id.*

D. Ramasubramani and Vuong Fail to Disclose All Elements of Claim 1

Applicant submits that *Ramasubramani* fails to disclose “said gaming server transmitting at least one of said plurality of keys over said network bus to said at least one gaming machine, said at least one gaming machine using said at least one of said plurality of keys to encrypt said information and said at least one gaming machine transmitting said encrypted information over said network bus to said remote machine,” as recited by Claim 1, as amended. In particular, the portions of *Ramasubramani* cited by the Examiner in his rejection actually describes prior art (to *Ramasubramani*) HTTPS communications between a client and a server, without the proxy server described in *Ramasubramani*. *Office Action* at 3 (citing *Ramasubramani*, col. 4, lines 29-50 and Figure 1, step 5). Thus, the cited portion of *Ramasubramani* fails to disclose that the proxy server (which the Examiner reads on the gaming server) transmits keys to the thin client (which the Examiner reads on the gaming machine).

Moreover, as noted above, *Ramasubramani* also fails to disclose “said at least one gaming machine using said at least one of said plurality of keys to encrypt said information and said at least one gaming machine transmitting said encrypted information over said network bus to said remote machine,” as recited by Claim 1, as amended. Rather, the proxy server communicates via the second protocol using the encryptions keys with a secure web server while communicating with the thin client via a different protocol. *Ramasubramani*, col. 12, lines 63 – col. 13, lines 1-11, col. 14, lines 18-41. Hence, not only does the cited portion of *Ramasubramani* fail to disclose the proxy server providing encryption keys to the thin client, there would be no need for such in the *Ramasubramani* system because the proxy server, not the thin client, encrypts communications with the secure web server (“the remote machine” in the Examiner’s terms). Rather, *Ramasubramani* discloses that the communications link between the proxy server and the thin client use a separate protocol, HDTP, a UDP protocol, from the HTTPS, a TCP protocol, that is used to communicate with the secure web server. *Ramasubramani*, col. 5, lines 47 – col. 6 line 10, and Figures 6A, 6B. Nowhere does the *Ramasubramani* indicate that the HDTP protocol uses either the keys or the certificates associated with the HTTPS communication with the secure web server to secure communications between the thin client and the secure web server, directly. *Ramasubramani*, col. 5, lines 47 – col. 6 line 10, and Figures 6A, 6B. In fact, Figure 6B and the accompanying description at col. 14, lines 18-42 disclose that it is the proxy server that encrypts

Appl. No. : 09/698507
Filed : October 26, 2000

the information exchanged between the thin client and the web site, and not the thin client. *Id.* at col. 12, line 64 – col. 13, line 11. Thus, *Ramasubramani* fails to teach or suggest a game machine receiving the keys from a server and using those keys to encrypt data to a remote machine. *Ramasubramani* fails to teach that the keys be transmitted from the proxy server to the thin client because it is the proxy server that both includes the keys and encrypts the communications with the secure web server. Similarly, *Ramasubramani* fails to teach or suggest that the thin client encrypt information using keys provided by the proxy server because the thin client first communicates information to the proxy server using HDTPT then the proxy server encrypts the encrypts and communicates with the secure web server using the keys.

Applicant further submits that nowhere does (and the Examiner does not so suggest that) *Vuong* teach or suggest “said gaming server transmitting at least one of said plurality of keys over said network bus to said at least one gaming machine, said at least one gaming machine using said at least one of said plurality of keys to encrypt said information and said at least one gaming machine transmitting said encrypted information over said network bus to said remote machine,” as recited by Claim 1, as amended. Accordingly, Applicant submits that as neither cited reference teaches or suggests such, Claim 1 is patentable for at least this reason.

E. No Motivation to Combine Has Been Shown

Not only do *Ramasubramani* and *Vuong* fail to disclose all elements of claim 1, Applicant submits that the Examiner has also failed to identify a proper motivation to combine these references. In particular, the Examiner argues that while *Ramasubramani* “does not specifically teach client and server to be a gaming machine and a gaming server,” it would have been obvious to combine *Ramasubramani* and *Vuong* because “gambling provides a euphoric feeling to users, with the added benefit of being able to play at home.”

Applicant submits that this finding does not support a *prima facie* rejection. Applicant submits that the prior art must suggest the desirability of the claimed invention. *See* M.P.E.P. § 2143.01. Applicant submits that merely because the references can be modified is not sufficient to establish *prima facie* obviousness. *Id.* Here, however, the Examiner has merely taken a generic (and, as noted above, inapplicable) encryption reference and made a conclusory finding that combining this system with a gaming system would provide a “euphoric feeling to users, with the added benefit of being able to play at home.” However, the Examiner provides no basis

Appl. No. : 09/698507
Filed : October 26, 2000

for why it would any more desirable for *Ramasubramani* to be combined with a gaming system such as *Vuong* as opposed to any other system known to provide a euphoric feeling to users.

Moreover, *Vuong* itself discloses a gaming system that is capable of remote play. Thus, there would be no need to combine *Vuong* with *Ramasubramani* for “the added benefit of being able to play at home” because *Vuong* already provides the benefit identified by the Examiner.

In addition, nowhere does either *Vuong* or *Ramasubramani* disclose any suggestion for “said gaming server transmitting at least one of said plurality of keys over said network bus to said at least one gaming machine, said at least one gaming machine using said at least one of said plurality of keys to encrypt said information and said at least one gaming machine transmitting said encrypted information over said network bus to said remote machine,” as recited by Claim 1, as amended. Accordingly, Applicant submits that Claim 1 is not rendered obvious by the combination of *Vuong* with *Ramasubramani* because the references neither teach or suggest all limitations of Claim 1 and because there is no motivation, other than that found in Applicant’s own application, to combine these references. Applicant therefore requests that the rejection of Claim 1 under 35 U.S.C. § 103(a) be withdrawn.

F. Claims 2-70 Are Patentable For At Least the Same Reasons

Applicant further submits that independent Claims 17, 25, 38, 49, 55, 58, and 68 includes, at least, the patentable features of Claim 1, discussed above. Therefore, for at least the reasons discussed in connection with Claim 1 above, Applicant submits that *Vuong* and *Ramasubramani*, alone and in combination, also fails to teach or suggest all elements of Claims 17, 25, 38, 49, 55, 58, and 68. Accordingly, Applicant submits that those claims are also patentable. Furthermore, as each of Claims 2-16, 18-24, 39-48, 50-54, 56-57, and 59-67, and 69-70 depend from one of Claims 17, 25, 38, 49, 55, 58, and 68, Applicant submits that f Claims 2-16, 18-24, 39-48, 50-54, 56-57, and 59-67, and 69-70 are patentable for at least the same reasons.

III. Conclusion

Applicant has endeavored to address all of the Examiner’s concerns as expressed in the Office Action. Accordingly, amendments to the claims, the reasons therefor, and arguments in support of patentability of the pending claim set are presented above. Any claim amendments which are not specifically discussed in the above remarks are made in order to improve the clarity of claim language, to correct grammatical mistakes or ambiguities, and to otherwise

Appl. No. : 09/698507
Filed : October 26, 2000

improve the clarity of the claims to particularly and distinctly point out the invention to those of skill in the art. Finally, Applicant submits that the claim limitations above represent only illustrative distinctions. Hence, there may be other patentable features that distinguish the claimed invention from the prior art.

In view of the foregoing, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections and, particularly, that all claims be allowed. If the Examiner finds any remaining impediment to the prompt allowance of these claims that could be clarified with a telephone conference, the Examiner is respectfully invited to call the undersigned. Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: October 26, 2000

By: JR

John Rickenbrode
Registration No. 57,067
Attorney of Record
Customer No. 20,995
(619) 235-8550

2256313-gem010306